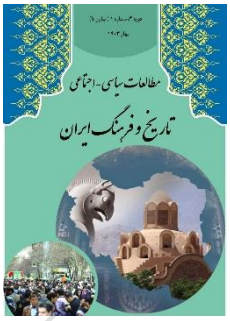
Journal Website

Article history:
Received 03 January 2025
Revised 26 February 2025
Accepted 12 March 2025
Published online 17 October 2025

Journal of Social-Political Studies of Iran's Culture and History

In Press



Cyber Warfare and Its Consequences for Iran's National Security

Behrouz. Nasiri[1], Ghasem. Torabi[2*], Alireza. Rezaei[2]

[1] PhD Student of International Relations, Hamedan Branch, Islamic Azad University, Hamedan, Iran
[2] Associate Professor of International Relations, Hamedan Branch, Islamic Azad University, Hamedan, Iran

*** Corresponding author email address**: ghasemtoraby@yahoo.com

A r t i c l e I n f o

Article type:
Original Research

How to cite this article:
Nasiri, B., Torabi, G., & Rezaei, A. (IN PRESS). Cyber Warfare and Its Consequences for Iran's National Security. *Journal of Social-Political Studies of Iran's Culture and History*.

© 2024 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

A B S T R A C T

In recent years, cybersecurity has become one of the strategic dimensions of national security. With the expansion of cyberattacks and the increasing complexity of penetration methods, cyber threats have affected not only information security but also critical infrastructure, the economy, national defense, and public opinion in various countries. Over the past two decades, the Islamic Republic of Iran has been targeted by numerous attacks, including the Stuxnet and Flame malware, financial system intrusions, and disruptions to critical infrastructure such as transportation and energy. This study, employing a descriptive-analytical method and based on qualitative research, examines the consequences of these attacks on Iran's national security and analyzes the existing challenges in this domain. The findings indicate that weaknesses in institutional coordination, dependence on foreign technologies, and the absence of a comprehensive national policy framework have increased Iran's cyber vulnerabilities. In this regard, the study proposes several countermeasures, including the formulation of a comprehensive cybersecurity strategy, the strengthening of indigenous infrastructure, the expansion of international cooperation, and the establishment of a National Cybersecurity Coordination Center. Without the adoption of preventive and coordinated measures, cyber threats could become one of the most significant security challenges for Iran in the coming years.

Keywords: *Cybersecurity, Cyberattacks, Information Warfare, Critical Infrastructure, Iran's National Security.*

PROOF VERSION

EXTENDED ABSTRACT

The rise of cyber warfare has significantly reshaped the nature of national security threats in the 21st century. Unlike conventional military conflicts, cyber warfare does not require physical force but relies on digital infiltration, network disruption, and information manipulation to weaken adversaries. This has made cyberspace a crucial battleground for both state and non-state actors, transforming traditional security strategies. Iran, due to its geopolitical significance and strategic infrastructure, has been a frequent target of cyberattacks orchestrated by foreign governments and independent hacker groups. Some of the most notable cyber incidents against Iran include the Stuxnet attack in 2010, which targeted its nuclear facilities, and subsequent cyber campaigns aimed at financial institutions, energy infrastructure, and communication networks (Buzan, 1991). The complexity of cyber threats has forced Iran to rethink its national security policies and implement defensive measures to counteract these evolving risks (Torabi, 2018). However, the country's dependency on foreign technologies, inadequate institutional coordination, and absence of a unified cybersecurity framework continue to expose vulnerabilities within its national security infrastructure (Rosenau, 2011). Given the growing sophistication of cyberattacks and their potential to disrupt economic, political, and defense systems, cyber warfare is now considered one of the most pressing security challenges facing the Iranian government (Brenner & Clarke, 2010).

Theoretical perspectives on cyber warfare vary widely, reflecting different interpretations of power dynamics in cyberspace. From a realist standpoint, cyber warfare is perceived as an extension of state power, where nations deploy cyberattacks to assert dominance over their adversaries (Buzan, 1991). Realist scholars argue that cyberspace, much like traditional battlefields, is governed by power struggles, where stronger nations exploit digital vulnerabilities to weaken their geopolitical rivals (Hare, 2010). Liberal theorists, in contrast, emphasize the role of international cooperation and regulatory frameworks in mitigating cyber threats (Krishnasamy & Venkatachalam, 2021). They advocate for collaborative cybersecurity initiatives, highlighting agreements such as the Budapest Convention on Cybercrime, which seeks to establish global standards for combating cybercriminal activities (Eriksson & Giacomello, 2006). Meanwhile, constructivist scholars focus on the socio-political implications of cyber warfare, arguing that digital conflicts are not just technical but also deeply rooted in ideological struggles and identity politics (Starr, 2009). The Iranian case exemplifies how cyber warfare is employed both as a tactical tool for espionage and disruption and as a strategic mechanism for shaping public perception and controlling narratives (Rosenau, 2011). These theoretical insights underscore the multifaceted nature of cyber warfare, demonstrating that its impact extends beyond the digital realm to influence national policies, global diplomacy, and even societal structures (Buzan, 1999).

Iran has experienced numerous cyberattacks against its critical infrastructure, ranging from energy facilities to financial institutions. The Stuxnet attack in 2010, widely attributed to the United States and Israel, was the first known instance of a cyber weapon being used to physically damage an industrial system (Talebpour, 2019). This attack demonstrated the potential of cyber warfare to cripple national security assets without direct military confrontation (Sayyad et al., 2020). Subsequent attacks, such as the Flame malware and Shamoon virus, have targeted Iranian energy networks and government agencies, leading to substantial data breaches and operational disruptions (Ahmadinejad, 2010). Iran's financial sector has also been subjected to cyber assaults, including denial-of-service (DDoS) attacks on major banks, aimed at destabilizing the national economy (Abdollah Khani, 2003). The increasing frequency and

PROOF VERSION

sophistication of these cyberattacks have underscored the urgent need for robust cybersecurity policies and infrastructure resilience (Torabi, 2018). However, Iran's cybersecurity landscape is hindered by systemic challenges, including insufficient investment in indigenous technology development, limited expertise in cybersecurity threat mitigation, and weak legal frameworks governing digital defense strategies (Brenner & Clarke, 2010). These challenges highlight the need for a comprehensive cybersecurity strategy that integrates defensive, offensive, and regulatory measures to safeguard national security interests (Baman Eghbali Zarch, 2022).

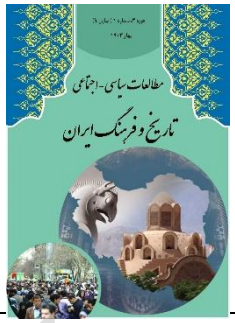
Cyber warfare not only threatens national security infrastructure but also has far-reaching economic and political consequences. The disruption of financial systems, interference with communication networks, and targeted attacks on industrial control systems can significantly undermine national stability (Buzan, 1999). In recent years, cyberattacks against Iranian energy infrastructure, including oil and gas facilities, have resulted in temporary shutdowns and operational setbacks, affecting domestic energy production and exports (Talebpour, 2019). Similarly, cyber incidents targeting Iran's transportation sector, such as railway system disruptions, have demonstrated the vulnerability of public service networks to digital sabotage (Sayyad et al., 2020). Beyond economic implications, cyber warfare also serves as a tool for political coercion and psychological operations, where misinformation campaigns and cyber espionage are used to manipulate public opinion and destabilize governance structures (Rosenau, 2011). Social media platforms, in particular, have become battlegrounds for cyber influence operations, where foreign actors deploy disinformation strategies to incite social unrest and erode public trust in governmental institutions (Ahmadinejad, 2010). These digital threats necessitate a multidimensional response that includes not only technological advancements but also legal and diplomatic efforts to combat cybercrime and cyberterrorism (Krishnasamy & Venkatachalam, 2021). As cyber warfare continues to evolve, Iran must prioritize the development of cyber deterrence mechanisms, invest in cybersecurity training programs, and foster international collaborations to enhance its cyber resilience (Baman Eghbali Zarch, 2022).

To counter cyber threats, Iran has undertaken various measures aimed at strengthening its digital defense capabilities. One of the most significant initiatives in this regard is the establishment of the National Information Network (NIN), designed to reduce reliance on foreign internet infrastructure and enhance national cybersecurity sovereignty (Sayyad et al., 2020). Additionally, Iran has expanded its cybersecurity workforce, investing in training programs for IT professionals and cybersecurity experts to bolster its cyber defense strategies (Torabi, 2018). Government agencies have also introduced cybersecurity legislation to regulate online activities, prevent unauthorized access to sensitive data, and deter cybercriminal activities (Buzan, 1999). Despite these efforts, challenges remain in ensuring a cohesive national cybersecurity strategy that integrates public and private sector initiatives (Cassese, 2005). The lack of coordination among governmental institutions, the absence of a centralized cyber command structure, and the persistent reliance on outdated security protocols continue to pose significant obstacles to Iran's cybersecurity preparedness (Brenner & Clarke, 2010). Moving forward, Iran must adopt a proactive approach to cybersecurity, incorporating threat intelligence sharing mechanisms, fostering research and development in cybersecurity innovation, and engaging in diplomatic efforts to establish global cybersecurity norms (Buzan, 1991).

PROOF VERSION

In conclusion, cyber warfare represents a critical and evolving threat to Iran's national security, requiring a comprehensive and adaptive response. The increasing sophistication of cyberattacks, their potential to disrupt critical infrastructure, and their role in economic and political destabilization necessitate a holistic approach to cybersecurity. Iran's experience with cyber warfare has demonstrated the need for investment in indigenous technological capabilities, the development of a cohesive national cybersecurity strategy, and enhanced international cooperation to address digital threats. The integration of cyber resilience into national defense policies, alongside efforts to strengthen legal and regulatory frameworks, will be essential in mitigating cyber risks. Moreover, fostering public awareness and digital literacy is crucial in combating misinformation campaigns and cyber manipulation tactics. As cyber warfare continues to shape global security dynamics, Iran must remain vigilant in safeguarding its digital sovereignty and fortifying its national cybersecurity infrastructure. Without a proactive and coordinated effort, cyber threats will continue to pose significant challenges to Iran's security landscape in the coming years.

PROOF VERSION



مطالعات سیاسی–اجتماعی تاریخ و فرهنگ ایران

در دست چاپ

وبسایت مجله

تاریخچه مقاله
دریافت شده در تاریخ ۱۴ دی ۱۴۰۳
اصلاح شده در تاریخ ۸ اسفند ۱۴۰۳
پذیرفته شده در تاریخ ۲۲ اسفند ۱۴۰۳
منتشر شده در تاریخ ۲۵ مهر ۱۴۰۴

جنگ سایبری و پیامدهای آن برای امنیت ملی ایران

بهروز نصیری[۱]، قاسم ترابی[۲*]، علیرضا رضایی[۲]

۱. دانشجوی دکتری تخصصی روابط بین الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران
۲. دانشیار روابط بین الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران

***ایمیل نویسنده مسئول:** ghasemtoraby@yahoo.com

اطلاعات مقاله

نوع مقاله
پژوهشی اصیل

نحوه استناد به این مقاله:
نصیری، بهروز.، ترابی، قاسم.، و رضایی، علیرضا. (در دست چاپ). جنگ سایبری و پیامدهای آن برای امنیت ملی ایران. *مطالعات سیاسی-اجتماعی تاریخ و فرهنگ ایران*.

© ۱۴۰۳ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

چکیده

امنیت سایبری در سال‌های اخیر به یکی از ابعاد راهبردی امنیت ملی تبدیل شده است. با گسترش حملات سایبری و پیچیدگی فزاینده روش‌های نفوذ، تهدیدات سایبری نه تنها امنیت اطلاعات، بلکه زیرساخت‌های حیاتی، اقتصاد، دفاع ملی و افکار عمومی کشورها را نیز تحت تأثیر قرار داده اند. جمهوری اسلامی ایران طی دو دهه اخیر، هدف حملات متعددی از جمله بدافزارهای استاکس نت و شعله، نفوذ به سامانه‌های مالی و اختلال در زیرساخت‌های حیاتی مانند حمل ونقل و انرژی قرار گرفته است. پژوهش حاضر با استفاده از روش توصیفی-تحلیلی و بر مبنای مطالعه کیفی، به بررسی پیامدهای این حملات بر امنیت ملی ایران پرداخته و چالش‌های موجود در این حوزه را تحلیل کرده است. یافته‌های تحقیق نشان می‌دهد که ضعف در هماهنگی نهادی، وابستگی به فناوری‌های خارجی و خلأ سیاست گذاری ملی، آسیب پذیری سایبری کشور را افزایش داده است. در این راستا، تدوین راهبرد جامع امنیت سایبری، تقویت زیرساخت‌های بومی، توسعه همکاری‌های بین المللی و ایجاد مرکز ملی هماهنگی امنیت سایبری به عنوان راهکارهای پیشنهادی ارائه شده اند. بدون اتخاذ تدابیر پیشگیرانه و هماهنگ، تهدیدات سایبری می‌توانند به یکی از مهم ترین چالش‌های امنیتی ایران در سال‌های آینده تبدیل شوند.

کلیدواژگان: *امنیت سایبری، حملات سایبری، جنگ اطلاعاتی، زیرساخت‌های حیاتی، امنیت ملی ایران.*

PROOF VERSION

مقدمه

امنیت ملی در عصر دیجیتال با چالش‌های نوظهوری روبه رو شده است که تهدیدات سایبری در صدر آن‌ها قرار دارد. پیشرفت فناوری اطلاعات و گسترش فضای سایبری، هرچند امکان توسعه اقتصادی، ارتباطات بین المللی و بهبود زیرساخت‌های امنیتی را فراهم کرده، اما همزمان زمینه ساز افزایش تهدیدات امنیتی نیز شده است (Buzan, 1999). جنگ سایبری به عنوان یکی از مهم ترین مؤلفه‌های تهدیدات سایبری، با هدف اختلال در زیرساخت‌های حیاتی، سرقت اطلاعات، جاسوسی و برهم زدن نظام‌های امنیتی کشورها طراحی می‌شود و ایران از جمله کشورهایی است که بیشترین تهدیدات را در این حوزه تجربه کرده است (Castells, 2010). ماهیت جنگ سایبری با جنگ‌های سنتی تفاوت اساسی دارد. در جنگ‌های سنتی، بازیگران عمدتاً دولت‌ها و گروه‌های نظامی هستند و مرزهای مشخصی برای درگیری‌های مسلحانه وجود دارد، اما در جنگ سایبری، نه تنها دولت ها، بلکه گروه‌های غیردولتی، تروریست‌ها و حتی هکرهای مستقل نیز می‌توانند نقش آفرین باشند (Torabi, 2018). این مسئله سبب تغییر مفهوم امنیت ملی شده و کشورها را مجبور به بازنگری در سیاست‌های دفاعی خود کرده است (Rosenau, 2011).

در دنیای امروز، جنگ سایبری به عنوان یکی از تهدیدات راهبردی علیه امنیت ملی کشورها شناخته می‌شود. این نوع جنگ، که به سرعت در حال گسترش است، تأثیرات عمیقی بر زیرساخت‌های امنیتی و اطلاعاتی کشورها گذاشته و موجب تغییر در راهبردهای دفاعی و امنیتی دولت‌ها شده است (Buzan, 1999). ایران نیز از جمله کشورهایی است که به دلیل موقعیت ژئوپلیتیکی و اهمیت استراتژیک، در معرض تهدیدات فزاینده‌ای از سوی بازیگران دولتی و غیردولتی در فضای سایبری قرار دارد (Torabi, 2018). با توجه به رشد روزافزون تهدیدات سایبری، ضرورت اتخاذ سیاست‌های امنیتی جدید برای محافظت از زیرساخت‌های حیاتی کشور بیش از پیش احساس می‌شود. جمهوری اسلامی ایران، با درک اهمیت جنگ سایبری، به دنبال توسعه قابلیت‌های دفاعی خود در این حوزه بوده و تلاش دارد تا با تقویت ساختارهای امنیتی، از حملات سایبری جلوگیری کند. با این حال، برای مقابله مؤثر با تهدیدات سایبری، لازم است که همکاری‌های بین المللی افزایش یافته، آموزش نیروی انسانی متخصص تقویت شده و زیرساخت‌های امنیتی داخلی بهبود یابد (Torabi, 2018).

در سال‌های اخیر، ایران یکی از اهداف اصلی حملات سایبری بوده است و حملات گسترده‌ای علیه زیرساخت‌های حیاتی این کشور انجام شده است. از مهم ترین این حملات می‌توان به ویروس استاکس نت اشاره کرد که در سال ۲۰۱۰ با هدف تخریب تأسیسات هسته‌ای ایران طراحی شد و آسیب‌های جدی به سانتریفیوژهای غنی سازی اورانیوم وارد کرد (Talebpour, 2019). این حمله به عنوان یکی از اولین نمونه‌های جنگ سایبری پیشرفته شناخته می‌شود که تأثیرات قابل توجهی بر برنامه هسته‌ای ایران داشت. علاوه بر این، حملات سایبری به سامانه‌های بانکی، زیرساخت‌های ارتباطی، سیستم‌های دفاعی و شبکه‌های اطلاعاتی ایران نیز در سال‌های اخیر افزایش یافته است (Sayyad et al., 2020). یکی از ویژگی‌های مهم جنگ سایبری، عدم شفافیت و پیچیدگی در شناسایی منابع تهدید است. در جنگ‌های متعارف، حمله کننده و هدف مشخص هستند، اما در حملات سایبری، ناشناس بودن مهاجم و دشواری در شناسایی منبع اصلی تهدید، مقابله با این حملات را چالش برانگیز کرده است (Ahmadinejad, 2010). در برخی موارد، دولت‌ها از گروه‌های هکری برای انجام حملات سایبری استفاده می‌کنند، به طوری که می‌توانند بدون پذیرش مسئولیت مستقیم، به اهداف خود دست یابند (Abdollah Khani, 2003). این مسئله سبب شده که بسیاری از حملات سایبری، به ویژه در مواردی که علیه ایران انجام شده، به بازیگران دولتی مانند آمریکا و اسرائیل نسبت داده شود (Torabi, 2018).

PROOF VERSION

تهدیدات سایبری نه تنها بر امنیت ملی، بلکه بر ثبات سیاسی، اقتصادی و اجتماعی کشورها نیز تأثیر می‌گذارند. در ایران، حملات سایبری می‌توانند باعث ایجاد اختلال در سامانه‌های مالی، شبکه‌های ارتباطی و حتی افکار عمومی شوند (Buzan, 1999). به عنوان مثال، حمله به سامانه سوخت در سال ۱۴۰۰ که منجر به اختلال گسترده در توزیع بنزین در کشور شد، نمونه‌ای از تأثیرات اقتصادی و اجتماعی جنگ سایبری است. این حملات می‌توانند موجب ایجاد نارضایتی عمومی، کاهش اعتماد شهروندان به دولت و حتی بحران‌های امنیتی شوند (Rosenau, 2011). به دلیل پیچیدگی و گستردگی تهدیدات سایبری، استراتژی‌های سنتی امنیت ملی دیگر پاسخگوی این تهدیدات نیستند. به همین دلیل، کشورها در حال توسعه روش‌های نوین برای مقابله با جنگ سایبری و افزایش توانمندی‌های دفاعی خود هستند (Sayyad et al., 2020). در ایران نیز لازم است که راهبردهای جدیدی برای حفاظت از زیرساخت‌های حیاتی، ایجاد سیستم‌های دفاع سایبری پیشرفته و تقویت همکاری‌های بین المللی در حوزه امنیت سایبری اتخاذ شود (Ahmadinejad, 2010).

این تحقیق به بررسی چالش‌های جنگ سایبری و تأثیر آن بر امنیت ملی ایران پرداخته و به این پرسش اساسی پاسخ می‌دهد که چگونه تهدیدات سایبری، امنیت جمهوری اسلامی ایران را تحت تأثیر قرار می‌دهند؟ در این راستا، پژوهش حاضر تلاش می‌کند تا ابعاد مختلف تهدیدات سایبری را تحلیل کرده، مهم ترین حملات سایبری علیه ایران را بررسی کند و راهکارهای مناسبی برای مقابله با این تهدیدات ارائه دهد. همچنین، با بررسی نمونه‌های بین المللی، تلاش خواهد شد تا مقایسه‌ای میان سیاست‌های امنیت سایبری کشورهای مختلف انجام شده و پیشنهادهای کاربردی برای ارتقای سطح امنیت سایبری ایران ارائه شود.

تأثیر جنگ سایبری بر زیرساخت‌های امنیتی و اطلاعاتی

زیرساخت‌های امنیتی و اطلاعاتی هر کشور یکی از مهم ترین ارکان حفظ حاکمیت ملی و ثبات سیاسی محسوب می‌شود. حملات سایبری با هدف تخریب این زیرساخت ها، نه تنها می‌توانند موجب اختلال در عملکرد دولت شوند، بلکه حتی می‌توانند باعث فروپاشی سیستم‌های حیاتی کشور گردند (Castells, 2010). در سال‌های اخیر، حملات سایبری متعددی علیه ایران انجام شده است که هدف آن ها، تضعیف توانمندی‌های اطلاعاتی و زیرساخت‌های امنیتی کشور بوده است. نمونه‌ای از این حملات، حمله استاکس نت در سال ۲۰۱۰ بود که با هدف از کار انداختن تأسیسات غنی سازی اورانیوم در نطنز صورت گرفت. این حمله، که به طور مشترک توسط ایالات متحده و اسرائیل طراحی شده بود، باعث ایجاد اختلال جدی در فرآیند غنی سازی اورانیوم و کاهش توان عملیاتی سانتریفیوژهای ایران شد (Talebpour, 2019). این حمله نشان داد که جنگ سایبری می‌تواند به عنوان یک ابزار جنگی واقعی، علیه زیرساخت‌های حیاتی یک کشور مورد استفاده قرار گیرد (Sayyad et al., 2020).

علاوه بر تهدیدات فیزیکی، حملات سایبری می‌توانند به عنوان ابزاری برای جنگ اطلاعاتی نیز به کار گرفته شوند. در سال‌های اخیر، جنگ اطلاعاتی از طریق عملیات‌های نفوذ سایبری، انتشار اخبار جعلی و دستکاری اطلاعات استراتژیک در فضای مجازی به یکی از چالش‌های مهم دولت‌ها تبدیل شده است (Rosenau, 2011). در ایران، حملات سایبری به سیستم‌های دولتی، نهادهای امنیتی و حتی رسانه‌های رسمی با هدف تغییر افکار عمومی و ایجاد نارضایتی اجتماعی انجام شده است (Ahmadinejad, 2010). این مسئله تأثیر مستقیمی بر امنیت ملی داشته و دولت‌ها را مجبور به توسعه سیاست‌های جدید امنیت سایبری کرده است (Abdollah Khani, 2003).

رشد تهدیدات سایبری و تأثیر آن بر سیاست‌های دفاعی ایران

با افزایش توانایی‌های بازیگران سایبری و گسترش تهدیدات سایبری، دولت‌ها ناچار به تغییر سیاست‌های دفاعی خود شده اند. ایران، که در سال‌های اخیر هدف حملات سایبری متعددی از سوی ایالات متحده، اسرائیل و گروه‌های تروریستی قرار گرفته است، در حال توسعه سیاست‌های دفاع سایبری خود برای مقابله با این تهدیدات است (Baman Eghbali Zarch, 2022). در همین راستا، جمهوری اسلامی ایران

PROOF VERSION

با ایجاد مرکز فرماندهی دفاع سایبری، توسعه زیرساخت‌های امنیت سایبری و افزایش توانایی‌های دفاعی در برابر حملات الکترونیکی، گام‌های مهمی برای کاهش آسیب پذیری‌های خود برداشته است (Sayyad et al., 2020). با این حال، چالش‌های متعددی همچنان در مسیر مقابله با این تهدیدات وجود دارد، از جمله وابستگی به زیرساخت‌های خارجی، کمبود نیروهای متخصص در حوزه امنیت سایبری و ضعف در هماهنگی میان نهادهای امنیتی کشور (Torabi, 2018).

یکی از مهم ترین چالش‌های پیش روی سیاست‌های دفاعی ایران، عدم قطعیت در شناسایی مهاجمان سایبری و دشواری در انتساب حملات است. بسیاری از حملات سایبری، به ویژه آن‌هایی که علیه زیرساخت‌های حیاتی ایران صورت گرفته اند، به بازیگران دولتی مانند ایالات متحده و اسرائیل نسبت داده شده اند، اما شواهد قطعی برای اثبات این ادعاها اغلب در دسترس نیست (Rosenau, 2011). این مسئله باعث شده است که ایران در برخی موارد، نتواند اقدامات حقوقی و دیپلماتیک مناسبی برای مقابله با این تهدیدات اتخاذ کند (Talebpour, 2019). با توجه به این تهدیدات، سیاست‌های دفاعی ایران در حوزه سایبری بر افزایش بازدارندگی سایبری، تقویت همکاری‌های منطقه‌ای و بین المللی و توسعه فناوری‌های بومی در حوزه امنیت سایبری متمرکز شده است (Buzan, 1999). راه اندازی شبکه ملی اطلاعات و کاهش وابستگی به سرویس‌های اینترنتی خارجی نیز یکی از راهبردهای مهم ایران برای مقابله با تهدیدات سایبری محسوب می‌شود (Sayyad et al., 2020).

مبانی نظری

رویکردهای نظری مرتبط با تهدیدهای سایبری

الف) رویکرد واقع گرایی (Realism)

مطابق دیدگاه واقع گرایان، تهدیدات سایبری بخشی از رقابت قدرت میان دولت‌ها محسوب می‌شوند. از این منظر، کشورها از فضای سایبری به عنوان یک ابزار برای افزایش قدرت، جمع آوری اطلاعات و مقابله با دشمنان خود استفاده می‌کنند (Buzan, 1991). طبق این رویکرد، جنگ سایبری می‌تواند ابزاری برای تضعیف توانایی‌های نظامی و اقتصادی رقبا باشد، بدون آنکه منجر به یک جنگ متعارف شود (Hare, 2010). مطالعات انجام شده در این زمینه نشان می‌دهند که ایالات متحده و کشورهای غربی از راهبردهای سایبری برای محدودسازی نفوذ کشورهای در حال توسعه مانند ایران، چین و روسیه استفاده کرده‌اند (Kizza, 2007).

ب) رویکرد لیبرالیسم (Liberalism)

لیبرال‌ها بر این باورند که امنیت سایبری یک مسئله بین المللی است و همکاری میان دولت‌ها و سازمان‌های فراملی، نقش کلیدی در مقابله با تهدیدات سایبری دارد (Eriksson & Giacomello, 2006). از این منظر، استانداردهای بین المللی، همکاری‌های امنیتی و نهادهای فراملی می‌توانند نقشی کلیدی در تنظیم فضای سایبری و مقابله با تهدیدات آن داشته باشند (Krishnasamy & Venkatachalam, 2021). این دیدگاه به ویژه در تدوین پیمان‌های بین المللی مرتبط با امنیت سایبری، مانند کنوانسیون بوداپست، تأثیرگذار بوده است.

ج) دیدگاه سازه انگاری (Constructivism)

از نگاه سازه انگاران، فضای سایبری تنها یک بستر فنی نیست، بلکه یک محیط اجتماعی و فرهنگی است که هویت دولت‌ها و ملت‌ها را نیز تحت تأثیر قرار می‌دهد (Rosenau, 2011). در این راستا، تهدیدات سایبری می‌توانند با استفاده از جنگ اطلاعاتی و تأثیرگذاری بر افکار عمومی، مشروعیت دولت‌ها را کاهش دهند (Starr, 2009). حملات سایبری به رسانه‌ها و انتشار اطلاعات جعلی در بسترهای آنلاین، می‌توانند تأثیرات گسترده‌ای بر امنیت ملی و اجتماعی کشورها داشته باشند (Talebpour, 2019).

تعریف و مفاهیم امنیت سایبری

PROOF VERSION

امنیت سایبری به عنوان یک حوزه میان رشته ای، شامل تدابیری است که برای محافظت از اطلاعات، شبکه ها، سیستم‌ها و زیرساخت‌های دیجیتال در برابر حملات و تهدیدات سایبری طراحی شده‌اند (Buzan, 1991). در سال‌های اخیر، مفهوم امنیت سایبری فراتر از محافظت از داده‌ها و سیستم‌های اطلاعاتی رفته و ابعاد جدیدی همچون امنیت اقتصادی، اجتماعی و حتی امنیت ملی را در بر گرفته است (Ahmed Jamal, 2021).

مطالعات انجام شده در این حوزه نشان می‌دهند که امنیت سایبری از چند بعد قابل بررسی است:

۱. امنیت اطلاعات: محافظت از داده‌های حیاتی کشورها در برابر دسترسی‌های غیرمجاز و حملات سایبری (Liu et al., 2021).

۲. امنیت شبکه: پیشگیری از حملات به شبکه‌های ارتباطی و زیرساخت‌های حیاتی (Krishnasamy & Venkatachalam, ۲۰۲۱:۱۰).

۳. امنیت زیرساخت‌های دیجیتال: حفاظت از سیستم‌های کنترل صنعتی و زیرساخت‌های استراتژیک کشور (Baman Eghbali Zarch, 2022).

۴. امنیت افکار عمومی و اطلاعاتی: مقابله با جنگ اطلاعاتی و انتشار اخبار جعلی که می‌توانند ثبات ملی را تهدید کنند (Rosenau, 2011).

در ایران، امنیت سایبری به یکی از اولویت‌های راهبردی کشور تبدیل شده است و دولت تلاش دارد با تقویت زیرساخت‌های دفاع سایبری و راه اندازی شبکه ملی اطلاعات، آسیب پذیری کشور را کاهش دهد (Torabi, 2018).

دامنه حملات سایبری

حملات سایبری را می‌توان به سه دسته کلی تقسیم کرد:

۱. حملات سایبری علیه زیرساخت‌های حیاتی

یکی از مهم ترین تهدیدات سایبری، حمله به زیرساخت‌های حیاتی کشورها مانند شبکه‌های برق، سامانه‌های کنترل صنعتی، سیستم‌های حمل ونقل و تأسیسات هسته‌ای است (Brenner & Clarke, 2010). حمله سایبری استاکس نت علیه تأسیسات هسته‌ای ایران در سال ۲۰۱۰، نمونه‌ای از این نوع حملات است که با هدف از کار انداختن تجهیزات سانتریفیوژها طراحی شد (Talebpour, 2019).

۲. حملات به سامانه‌های اطلاعاتی و بانکی

حملات به سامانه‌های بانکی و اطلاعاتی، می‌توانند موجب سرقت داده‌های مالی، اختلال در نظام اقتصادی و ایجاد بی ثباتی در بخش‌های مختلف کشور شوند (Alghamdi, 2021). در سال‌های اخیر، چندین حمله سایبری به بانک‌های ایرانی و شرکت‌های ارائه دهنده خدمات مالی صورت گرفته که خسارات سنگینی به بار آورده است (Baman Eghbali Zarch, 2022).

۳. حملات جنگ اطلاعاتی و انتشار اخبار جعلی

حملات سایبری تنها به تخریب فیزیکی محدود نمی‌شوند، بلکه جنگ اطلاعاتی و انتشار اخبار جعلی نیز یکی از ابزارهای تأثیرگذاری بر افکار عمومی و بی‌ثبات سازی کشورها است (Starr, 2009). انتشار اطلاعات نادرست در فضای مجازی و شبکه‌های اجتماعی، می‌تواند موجب کاهش اعتماد عمومی به نهادهای دولتی و افزایش تنش‌های اجتماعی شود (Rosenau, 2011).

روش تحقیق

این پژوهش با بهره گیری از روش توصیفی-تحلیلی و بر اساس مطالعات کیفی و اسنادی انجام شده است. هدف اصلی این تحقیق، تحلیل نظام مند تهدیدات سایبری و تأثیر آن‌ها بر امنیت ملی جمهوری اسلامی ایران، همراه با بررسی سیاست‌های دفاعی و راهکارهای مقابله‌ای

PROOF VERSION

است. به منظور دستیابی به این هدف، پژوهش حاضر ضمن مطالعه تطبیقی حملات سایبری در سطح بین المللی، به تحلیل حملات سایبری شاخص علیه ایران پرداخته است. نمونه‌های بررسی شده شامل حملات استاکس نت (۲۰۱۰)، شعله (۲۰۱۲)، نفوذ به سامانه‌های بانکی (۲۰۱۸) و حملات به زیرساخت‌های حیاتی همچون سامانه توزیع سوخت (۱۴۰۰) هستند. این نمونه‌ها به طور هدفمند انتخاب شده اند، زیرا دارای اثرات راهبردی بر امنیت ملی ایران بوده و موجب تغییر در سیاست‌های سایبری کشور شده اند. به منظور تقویت یافته‌های پژوهش، نمونه‌های تطبیقی از کشورهای دیگر نظیر چین و روسیه نیز مورد بررسی قرار گرفته است.

جامعه آماری پژوهش شامل کلیه اسناد، گزارش‌ها و مطالعات علمی معتبر در حوزه امنیت سایبری است که از طریق روش نمونه گیری هدفمند انتخاب شده اند. نحوه گردآوری اطلاعات بر مبنای تحلیل منابع علمی، گزارش‌های امنیتی، اسناد بین المللی و داده‌های منتشرشده توسط نهادهای مرتبط از جمله شورای عالی فضای مجازی، سازمان پدافند غیرعامل و مجامع بین المللی مانند سازمان همکاری شانگهای صورت گرفته است. به منظور افزایش دقت و صحت تحلیل ها، از روش مقایسه‌ای برای تطبیق داده‌های مربوط به تهدیدات سایبری ایران با نمونه‌های بین المللی استفاده شده است. علاوه بر این، داده‌های آماری مرتبط با میزان حملات سایبری، روش‌های نفوذ و تأثیر آن‌ها بر زیرساخت‌های ملی، برای تکمیل تحلیل‌های کیفی مورد استفاده قرار گرفته اند. به کارگیری این چارچوب روش شناختی، امکان ارائه تصویری جامع و دقیق از وضعیت امنیت سایبری ایران و راهکارهای مؤثر برای مقابله با تهدیدات در این حوزه را فراهم کرده است.

تجزیه و تحلیل

تهدیدات و حملات سایبری

امنیت سایبری در دنیای امروز به یکی از مهم ترین دغدغه‌های دولت ها، نهادهای امنیتی و سازمان‌های بین المللی تبدیل شده است. افزایش وابستگی جوامع به فناوری‌های دیجیتال، شبکه‌های اطلاعاتی و سیستم‌های ارتباطی، موجب شده است که فضای مجازی نه تنها بستری برای توسعه و تعاملات بین المللی باشد، بلکه به یک میدان نبرد جدید برای تهدیدات امنیتی نیز تبدیل شود (Brenner & Clarke, 2010). تهدیدات سایبری به دلیل عدم وجود مرزهای فیزیکی و ناشناس بودن مهاجمان، نسبت به تهدیدات سنتی از پیچیدگی بیشتری برخوردارند و همین مسئله مقابله با آن‌ها را دشوارتر کرده است. با توجه به ماهیت این تهدیدات، آن‌ها را می‌توان در چهار دسته کلی شامل تهدیدات امنیتی فضای سایبر، جاسوسی سایبری، تروریسم سایبری و جنگ سایبری طبقه بندی کرد که هر یک پیامدهای متفاوتی بر امنیت ملی کشورها دارند (Buzan, 1991).

تهدیدات امنیتی فضای سایبر

تهدیدات امنیتی فضای سایبر، شامل هرگونه فعالیت مخرب در محیط دیجیتال است که هدف آن نفوذ به شبکه‌های اطلاعاتی، ایجاد اختلال در سیستم‌های حیاتی و تغییر یا تخریب داده‌ها می‌باشد (Beaumont, 2010). این نوع حملات معمولاً توسط گروه‌های هکری مستقل، سازمان‌های جرائم سایبری و در برخی موارد، دولت‌ها برای تضعیف دشمنان خود انجام می‌شوند. یکی از رایج ترین حملات در این حوزه، حملات منع سرویس توزیع شده (DDoS) است که با ارسال حجم بالایی از درخواست‌ها به یک سرور، موجب از کار افتادن خدمات حیاتی مانند سامانه‌های بانکی، دولتی و صنعتی می‌شود. در سال‌های اخیر، حملات منع سرویس گسترده‌ای علیه سامانه‌های ارتباطی و زیرساخت‌های حیاتی کشورهای مختلف صورت گرفته است. برای مثال، حملات سایبری علیه شبکه‌های مالی برخی کشورها، موجب قطع دسترسی میلیون‌ها کاربر به خدمات بانکی شده و خسارات اقتصادی قابل توجهی را به همراه داشته است. افزایش پیچیدگی این نوع تهدیدات، دولت‌ها را به سمت توسعه فناوری‌های امنیتی جدید از جمله هوش مصنوعی برای شناسایی الگوهای غیرعادی و جلوگیری از حملات سوق داده است (Baman Eghbali Zarch, 2022).

PROOF VERSION

جاسوسی سایبری

جاسوسی سایبری به فعالیت‌هایی اطلاق می‌شود که در آن، مهاجمان با هدف سرقت اطلاعات حساس، داده‌های دولتی، اطلاعات نظامی و اطلاعات مالی سازمان‌ها و نهادهای مختلف، اقدام به نفوذ به سامانه‌های دیجیتال می‌کنند.این نوع حملات معمولاً توسط دولت ها، سازمان‌های اطلاعاتی و گروه‌های هکری وابسته به آن‌ها انجام می‌شود که هدف اصلی آن‌ها جمع آوری اطلاعات محرمانه برای مقاصد استراتژیک است. یکی از مهم ترین چالش‌های مرتبط با جاسوسی سایبری، پیشرفته شدن روش‌های نفوذ و عدم امکان شناسایی سریع این نوع حملات است. مهاجمان می‌توانند بدون آنکه ردپایی از خود بر جای بگذارند، به سیستم‌های اطلاعاتی نفوذ کنند و داده‌های حساس را به طور پنهانی استخراج نمایند. بسیاری از کشورها برای مقابله با این نوع تهدیدات، اقدام به توسعه ابزارهای امنیتی پیشرفته مانند رمزگذاری داده‌ها و سامانه‌های چندلایه شناسایی نفوذ کرده‌اند (Buzan, 1991).

تروریسم سایبری

تروریسم سایبری یکی از تهدیدات نوظهوری است که در دهه‌های اخیر به شدت مورد توجه نهادهای امنیتی قرار گرفته است (Brenner & Clarke, 2010). تروریسم سایبری شامل فعالیت‌هایی است که گروه‌های تروریستی از طریق حملات سایبری برای تخریب زیرساخت‌های حیاتی، ایجاد وحشت عمومی و بی ثباتی سیاسی به کار می‌گیرند. این حملات می‌توانند علیه سامانه‌های کنترل صنعتی، شبکه‌های برق، سیستم‌های حمل ونقل و حتی رسانه‌های خبری انجام شوند.

در سال‌های اخیر، برخی از گروه‌های افراطی از فضای مجازی برای جذب نیرو، تأمین مالی و برنامه ریزی حملات سایبری علیه دولت‌ها استفاده کرده اند. این امر موجب شده است که کشورهای مختلف در سیاست‌های امنیتی خود، تمرکز بیشتری بر ردیابی فعالیت‌های سایبری گروه‌های تروریستی و توسعه راهکارهای نظارتی و کنترلی در فضای مجازی داشته باشند (Mandel, 2008).

تحلیل حملات سایبری علیه جمهوری اسلامی ایران

ایران طی دو دهه اخیر یکی از اهداف اصلی حملات سایبری در سطح بین المللی بوده است. این حملات که عمدتاً از سوی دولت‌های متخاصم و گروه‌های هکری وابسته به آن‌ها هدایت شده اند، تأثیرات قابل توجهی بر زیرساخت‌های حیاتی، امنیت اطلاعات و سیاست‌های دفاع سایبری کشور داشته اند. بررسی این حملات و تحلیل اثرات آن‌ها می‌تواند به درک بهتری از راهکارهای موردنیاز برای افزایش مقاومت سایبری کشور منجر شود. در این بخش، مهم ترین حملات سایبری علیه جمهوری اسلامی ایران، شامل حملات استاکس نت و شعله، حملات به زیرساخت‌های انرژی، حمل ونقل و اطلاعات، و تأثیر این حملات بر سیاست‌های دفاع سایبری کشور بررسی خواهد شد.

الف) حملات استاکس نت و شعله

حملات سایبری استاکس نت و شعله از مهم ترین و پیچیده ترین حملاتی هستند که تاکنون علیه زیرساخت‌های حیاتی جمهوری اسلامی ایران انجام شده اند. این حملات نه تنها خسارات فنی قابل توجهی را به تأسیسات هدف وارد کردند، بلکه موجب تغییر در راهبردهای دفاع سایبری ایران و توسعه برنامه‌های امنیتی جدید شدند.

۱. حمله استاکس نت (۲۰۱۰)

حمله استاکس نت یکی از اولین نمونه‌های شناخته شده از جنگ سایبری بود که با هدف تخریب برنامه هسته‌ای ایران طراحی و اجرا شد. این بدافزار که به صورت مشترک توسط ایالات متحده و اسرائیل توسعه یافته بود، توانست با نفوذ به سامانه‌های کنترل صنعتی تأسیسات هسته‌ای نطنز، تغییراتی در سرعت چرخش سانتریفیوژها ایجاد کرده و عملکرد آن‌ها را مختل کند. استاکس نت از طریق حافظه‌های USB آلوده به سیستم‌های صنعتی ایران منتقل شد و توانست بدون شناسایی، ماه‌ها در محیط‌های عملیاتی باقی بماند. این حمله نشان داد

PROOF VERSION

که چگونه بدافزارهای پیچیده می‌توانند به عنوان ابزاری برای ایجاد اختلال در زیرساخت‌های حیاتی یک کشور مورد استفاده قرار گیرند (Brenner & Clarke, 2010).

۲. حمله بدافزار شعله (۲۰۱۲)

پس از حمله استاکس نت، در سال ۲۰۱۲ بدافزار شعله (Flame) شناسایی شد که از آن به عنوان یکی از پیشرفته ترین ابزارهای جاسوسی سایبری یاد می‌شود. برخلاف استاکس نت که برای تخریب سخت افزاری طراحی شده بود، شعله با هدف سرقت اطلاعات حساس و جاسوسی دیجیتال مورد استفاده قرار گرفت. این بدافزار قادر بود مکالمات را ضبط کند، فعالیت‌های کیبوردی را ثبت کند، از صفحه نمایش اسکرین شات بگیرد و حتی داده‌های ذخیره شده را بدون جلب توجه منتقل کند. حمله شعله نشان داد که تهدیدات سایبری تنها محدود به ایجاد اختلال در زیرساخت‌های فیزیکی نیستند، بلکه می‌توانند تأثیرات گسترده‌ای بر امنیت اطلاعات و برنامه‌های محرمانه کشورها داشته باشند. هر دو حمله استاکس نت و شعله نقطه عطفی در تاریخ جنگ‌های سایبری محسوب می‌شوند و موجب شدند که ایران راهبردهای امنیتی خود را در این حوزه ارتقا دهد و سرمایه گذاری بیشتری بر توسعه قابلیت‌های دفاع سایبری و سیستم‌های تشخیص و پاسخ به تهدیدات سایبری انجام دهد (Buzan, 1991).

ب) حملات به زیرساخت‌های انرژی، حمل ونقل و اطلاعات

حملات سایبری علیه زیرساخت‌های حیاتی، از جمله شبکه‌های انرژی، حمل ونقل و اطلاعات، یکی از خطرناک ترین تهدیداتی است که می‌تواند امنیت ملی کشورها را به چالش بکشد. این حملات با هدف ایجاد اختلال در عملکرد سامانه‌های کلیدی و تضعیف توان مدیریتی و اجرایی دولت انجام می‌شوند. جمهوری اسلامی ایران طی سال‌های اخیر هدف چندین حمله سایبری گسترده علیه این زیرساخت‌ها قرار گرفته است که در این بخش به بررسی مهم ترین آن‌ها پرداخته می‌شود.

۱. حملات به زیرساخت‌های انرژی

زیرساخت‌های انرژی به عنوان یکی از مهم ترین بخش‌های امنیت ملی، در برابر حملات سایبری آسیب پذیری بالایی دارند. هدف اصلی این نوع حملات، ایجاد اختلال در عرضه انرژی، مختل کردن تأسیسات تولید برق و نفت، و افزایش نارضایتی عمومی است.

یکی از نمونه‌های برجسته این حملات، حمله به تأسیسات نفتی ایران در سال ۲۰۱۸ بود که منجر به اختلال در برخی از سامانه‌های کنترلی تأسیسات نفت و گاز کشور شد. این حمله موجب شد که بخش‌هایی از سیستم‌های کنترلی به طور موقت از دسترس خارج شوند و برخی از عملیات‌های تولید و پالایش دچار وقفه شوند. هرچند این حمله به سرعت شناسایی و کنترل شد، اما نشان داد که بخش انرژی کشور یکی از اهداف استراتژیک مهاجمان سایبری است و نیاز به تقویت امنیت آن بیش از پیش احساس می‌شود (Brenner & Clarke, 2010).

۲. حملات به سیستم‌های حمل ونقل

حملات سایبری به سامانه‌های حمل ونقل می‌توانند پیامدهای امنیتی گسترده‌ای داشته باشند و موجب ایجاد بی ثباتی و اختلال در خدمات عمومی شوند. هدف این نوع حملات، از کار انداختن سیستم‌های مدیریت ترافیک، مختل کردن سامانه‌های مترو و قطار، و ایجاد بی نظمی در شبکه حمل ونقل شهری است.

در سال ۲۰۲۱، حمله سایبری گسترده‌ای علیه سامانه راه آهن ایران انجام شد که منجر به اختلال در سیستم‌های فروش بلیت و تأخیر در حرکت قطارها شد. مهاجمان سایبری در این حمله توانستند بخشی از اطلاعات مربوط به برنامه‌های حرکتی را تغییر دهند و با ایجاد بی نظمی در مدیریت سیستم، باعث اختلال در ارائه خدمات شوند. این حمله، اهمیت امنیت سایبری در زیرساخت‌های حمل ونقل کشور را بیش از پیش برجسته کرد و نشان داد که سامانه‌های هوشمند حمل ونقل نیز در برابر حملات سایبری آسیب پذیر هستند (Buzan, 1991).

PROOF VERSION

۳. حملات به شبکه‌های اطلاعات و ارتباطات

یکی از اصلی ترین اهداف حملات سایبری، نفوذ به شبکه‌های اطلاعاتی و ارتباطی کشور است که می‌تواند پیامدهای گسترده‌ای بر امنیت ملی و امنیت اطلاعاتی داشته باشد. این نوع حملات با هدف سرقت اطلاعات حساس، تغییر یا حذف داده ها، و از کار انداختن شبکه‌های ارتباطی انجام می‌شوند. در سال‌های اخیر، حملات متعددی علیه سامانه‌های دولتی و بانک‌های ایران انجام شده که منجر به افشای اطلاعات و مختل شدن برخی خدمات الکترونیکی شده است. نمونه‌ای از این حملات، حمله به سامانه‌های بانکی در سال ۲۰۱۹ بود که در آن، داده‌های مربوط به حساب‌های کاربران افشا شد و برخی از تراکنش‌های مالی به طور موقت دچار اختلال شدند.

ج) تأثیر این حملات بر سیاست‌های دفاع سایبری ایران

حملات سایبری گسترده علیه زیرساخت‌های حیاتی جمهوری اسلامی ایران، موجب تغییرات اساسی در راهبردهای دفاع سایبری کشور شده است. این حملات نشان داده اند که وابستگی به فناوری‌های دیجیتال، کشور را در برابر تهدیدات سایبری آسیب پذیر می‌کند و نیاز به توسعه سازوکارهای پیشرفته برای مقابله با این تهدیدات، بیش از پیش احساس می‌شود. در واکنش به این حملات، ایران اقدامات متعددی را برای تقویت امنیت سایبری خود اتخاذ کرده است که در ادامه بررسی می‌شود.

۱. توسعه شبکه ملی اطلاعات و کاهش وابستگی به اینترنت جهانی

یکی از نخستین واکنش‌های ایران به افزایش حملات سایبری، ایجاد و توسعه شبکه ملی اطلاعات (NIN) بود که با هدف کاهش وابستگی به اینترنت بین المللی و افزایش امنیت داده‌های داخلی طراحی شد. این شبکه امکان مدیریت بهتر داده ها، کنترل بیشتر بر جریان اطلاعات و جلوگیری از نفوذ بدافزارهای خارجی را فراهم می‌کند. اگرچه این طرح با چالش‌هایی در زمینه اجرا و هماهنگی میان نهادهای مختلف روبه رو بوده است، اما همچنان به عنوان یکی از مهم ترین راهبردهای دفاع سایبری کشور محسوب می‌شود (Baman Eghbali Zarch, 2022).

۲. راه اندازی و تقویت مراکز دفاع سایبری

در واکنش به حملات سایبری، ایران اقدام به ایجاد مراکز تخصصی دفاع سایبری از جمله مرکز ماهر (مدیریت امداد و هماهنگی رخدادهای رایانه ای) و افزایش ظرفیت‌های سازمان پدافند غیرعامل کرد. این مراکز نقش کلیدی در شناسایی تهدیدات سایبری، ارائه هشدارهای امنیتی و تقویت همکاری میان نهادهای دولتی برای مقابله با حملات سایبری دارند. ایران همچنین توانمندی‌های خود را در حوزه دفاع سایبری با توسعه نیروی انسانی متخصص و تقویت سامانه‌های شناسایی و پاسخگویی به تهدیدات ارتقا داده است (Cassese, 2005).

۳. افزایش همکاری‌های بین المللی در حوزه امنیت سایبری

با توجه به ماهیت فراملی تهدیدات سایبری، ایران تلاش کرده است که همکاری‌های بین المللی خود را در حوزه امنیت سایبری افزایش دهد. ایران با کشورهای عضو سازمان همکاری شانگهای و برخی کشورهای هم پیمان در زمینه تبادل اطلاعات، امنیت سایبری و ارتقای توانمندی‌های دفاعی، همکاری‌هایی داشته است. همچنین، اقدامات دیپلماتیک در راستای افزایش آگاهی جهانی از تهدیدات سایبری و ارائه پیشنهادهایی برای تنظیم مقررات بین المللی در این حوزه، در دستور کار سیاست گذاران ایرانی قرار گرفته است (Buzan, 1991).

تحلیل تأثیر تهدیدات سایبری بر امنیت ملی ایران

تهدیدات سایبری نه تنها به عنوان یک چالش فنی، بلکه به عنوان یک مسئله راهبردی که امنیت ملی کشور را در ابعاد مختلف تحت تأثیر قرار می‌دهد، مطرح شده است. حملات سایبری می‌توانند موجب اختلال در سامانه‌های دفاعی و نظامی، ایجاد بحران‌های اقتصادی،

PROOF VERSION

تضعیف زیرساخت‌های حیاتی و حتی تأثیرات عمیق بر افکار عمومی و امنیت اجتماعی شوند. با توجه به وابستگی فزاینده ایران به فناوری‌های دیجیتال، بررسی تأثیر این تهدیدات بر ابعاد مختلف امنیت ملی، امری ضروری است. در این بخش، اثرات تهدیدات سایبری بر امنیت نظامی، اقتصاد، زیرساخت‌های حیاتی و امنیت اجتماعی مورد تحلیل قرار می‌گیرد.

الف) تأثیر بر امنیت نظامی و دفاعی

امنیت نظامی و دفاعی، یکی از مهم ترین ابعاد امنیت ملی است که به شدت در معرض تهدیدات سایبری قرار دارد. با توجه به دیجیتالی شدن سامانه‌های نظامی، افزایش وابستگی به شبکه‌های ارتباطی و اتوماسیون دفاعی، نیروهای مسلح کشورها بیش از هر زمان دیگری در برابر حملات سایبری آسیب پذیر شده اند.

۱. نفوذ به سامانه‌های فرماندهی و کنترل نظامی

یکی از جدی ترین تهدیدات سایبری علیه امنیت نظامی، نفوذ به سامانه‌های فرماندهی و کنترل نیروهای مسلح است. حملات سایبری می‌توانند موجب تغییر یا تخریب داده‌های عملیاتی، مختل کردن ارتباطات نظامی و حتی کنترل از راه دور تجهیزات حساس شوند. چنین حملاتی می‌توانند در شرایط بحران، توانایی فرماندهی و تصمیم گیری نیروهای مسلح را به طور قابل توجهی کاهش دهند (Brenner & Clarke, 2010).

۲. حملات به سامانه‌های دفاع موشکی و پهپادی

سامانه‌های دفاعی مبتنی بر فناوری‌های پیشرفته، به شدت وابسته به سیستم‌های سایبری هستند. نفوذ به این سامانه‌ها می‌تواند موجب از کار افتادن یا تغییر مسیر موشک ها، ایجاد اختلال در عملکرد رادارهای هشداردهنده و حتی هک سامانه‌های پهپادی شود. در برخی موارد، مهاجمان سایبری توانسته اند با دستکاری داده‌های راداری، سیستم‌های دفاع هوایی را فریب دهند و مسیر عملیات‌های نظامی را تغییر دهند (Buzan, 1991).

۳. سرقت اطلاعات نظامی و جاسوسی سایبری

یکی از متداول ترین روش‌های حمله سایبری علیه نیروهای مسلح، نفوذ به شبکه‌های ارتباطی و پایگاه‌های داده نظامی برای سرقت اطلاعات محرمانه است. در سال‌های اخیر، موارد متعددی از تلاش برای نفوذ به سامانه‌های اطلاعاتی ایران با هدف دستیابی به اسناد دفاعی، برنامه‌های تسلیحاتی و اطلاعات عملیات‌های نظامی گزارش شده است. چنین حملاتی می‌توانند موجب افشای اطلاعات حساس و کاهش برتری استراتژیک کشور در حوزه دفاعی شوند (Cassese, 2005).

حملات سایبری علیه سامانه‌های نظامی، یکی از جدی ترین تهدیداتی است که می‌تواند امنیت دفاعی کشور را به شدت تحت تأثیر قرار دهد. نفوذ به سامانه‌های فرماندهی، کنترل تجهیزات نظامی و سرقت اطلاعات حساس، می‌تواند تأثیرات جبران ناپذیری بر توان دفاعی ایران داشته باشد. برای مقابله با این تهدیدات، ایران باید سرمایه گذاری بیشتری در حوزه امنیت سایبری نظامی انجام دهد، سامانه‌های ارتباطی خود را مقاوم سازی کند و همکاری‌های بین المللی برای تقویت توانمندی‌های دفاع سایبری را گسترش دهد (Beaumont, 2010).

ب) تهدیدات اقتصادی ناشی از جنگ سایبری

حملات سایبری تأثیرات مستقیمی بر اقتصاد ملی کشورها دارند و می‌توانند موجب اختلال در سامانه‌های مالی، کاهش اعتماد عمومی به بانکداری دیجیتال، سرقت اطلاعات مالی و ایجاد بی ثباتی در بازارهای اقتصادی شوند. با توجه به دیجیتالی شدن فعالیت‌های اقتصادی و افزایش وابستگی به شبکه‌های ارتباطی، آسیب پذیری اقتصادی کشورها در برابر تهدیدات سایبری افزایش یافته است. جمهوری اسلامی ایران نیز طی سال‌های اخیر هدف حملات سایبری گسترده‌ای قرار گرفته که خسارات قابل توجهی به بخش‌های مالی و اقتصادی وارد کرده است.

PROOF VERSION

۱. حملات به سامانه‌های بانکی و مالی

یکی از اصلی ترین اهداف حملات سایبری، زیرساخت‌های بانکی و سامانه‌های پرداخت الکترونیکی است. این حملات می‌توانند منجر به سرقت اطلاعات حساب‌های بانکی، تغییر در داده‌های مالی، ایجاد اختلال در خدمات آنلاین و حتی از بین رفتن سرمایه‌های کلان شوند. در سال‌های اخیر، چندین حمله سایبری علیه بانک‌های ایرانی انجام شده که در برخی موارد، منجر به افشای اطلاعات کاربران و مختل شدن تراکنش‌های مالی شده است. ایران در پاسخ به این تهدیدات، اقدام به افزایش امنیت شبکه‌های بانکی و توسعه سامانه‌های مقاوم سازی شده برای جلوگیری از نفوذهای سایبری کرده است.

۲. حملات به بازارهای مالی و بورس

بازارهای مالی و بورس نیز یکی از اهداف مهم حملات سایبری هستند، زیرا ایجاد اختلال در این حوزه می‌تواند موجب کاهش ارزش دارایی ها، سقوط شاخص‌های مالی و بی اعتمادی سرمایه گذاران شود. برخی از حملات سایبری با هدف تأثیرگذاری بر داده‌های معاملاتی، حذف یا تغییر اطلاعات بازار، و حتی متوقف کردن معاملات انجام شده اند. چنین حملاتی می‌توانند سرمایه گذاران را دچار سردرگمی کرده و موجب خروج سرمایه از بازارهای داخلی شوند که در نهایت به کاهش رشد اقتصادی کشور منجر خواهد شد.

۳. اخلال در زنجیره تأمین و تجارت الکترونیکی

حملات سایبری می‌توانند موجب اختلال در زنجیره تأمین کالاها و خدمات شوند. بسیاری از شرکت‌های بزرگ به سامانه‌های دیجیتال برای مدیریت موجودی، حمل ونقل و ارتباطات بین المللی وابسته هستند. حملات سایبری علیه این سامانه‌ها می‌توانند منجر به تأخیر در تحویل کالاها، کاهش بهره وری و افزایش هزینه‌های تولید شوند. در سال‌های اخیر، برخی از صنایع حساس ایران از جمله صنایع پتروشیمی و خودروسازی، هدف حملات سایبری قرار گرفته اند که موجب اختلال در روند تولید و توزیع شده است.

ج) آسیب پذیری زیرساخت‌های حیاتی

زیرساخت‌های حیاتی هر کشور شامل شبکه‌های انرژی، حمل ونقل، آب و فاضلاب، مخابرات، خدمات درمانی و مالی است که هرگونه اختلال در آن‌ها می‌تواند امنیت ملی را به طور جدی تهدید کند. حملات سایبری علیه این زیرساخت ها، می‌تواند موجب ایجاد بحران‌های گسترده و از کار افتادن خدمات اساسی شود که پیامدهای جبران ناپذیری برای کشور به همراه خواهد داشت. جمهوری اسلامی ایران نیز طی سال‌های اخیر هدف حملات متعددی علیه زیرساخت‌های حیاتی خود بوده که نشان دهنده آسیب پذیری این حوزه در برابر تهدیدات سایبری است.

۱. حملات سایبری به تأسیسات انرژی و نیروگاه ها

بخش انرژی، یکی از مهم ترین حوزه‌های زیرساختی کشور است که در برابر تهدیدات سایبری آسیب پذیر می‌باشد. حملات سایبری علیه تأسیسات نفتی، پالایشگاه‌ها و نیروگاه‌های برق می‌تواند موجب اختلال در تولید و توزیع انرژی شده و در نتیجه، عملکرد بسیاری از بخش‌های دیگر کشور را تحت تأثیر قرار دهد یکی از مهم ترین حملات سایبری علیه این حوزه، حمله به تأسیسات نفتی ایران در سال ۲۰۱۸ بود که موجب اختلال در برخی سامانه‌های کنترل صنعتی شد و توجه مقامات امنیتی را به لزوم افزایش امنیت سایبری در این بخش جلب کرد (Brenner & Clarke, 2010).

۲. حملات به سیستم‌های حمل ونقل و ترافیک شهری

PROOF VERSION

سیستم‌های حمل ونقل عمومی و مدیریت ترافیک، به شدت وابسته به فناوری‌های دیجیتال شده اند و همین امر آن‌ها را در برابر حملات سایبری آسیب پذیر کرده است. یک حمله موفق به سامانه‌های کنترل ترافیک یا سیستم‌های ریلی و هوایی، می‌تواند موجب ایجاد اختلالات گسترده و حتی خطرات جانی شود. حمله سایبری به سامانه راه آهن ایران در سال ۲۰۲۱ که موجب توقف برخی از قطارها و ایجاد ناهماهنگی در سیستم مدیریت راه آهن شد، نمونه‌ای از این نوع تهدیدات است که اهمیت افزایش سطح امنیت این زیرساخت‌ها را برجسته کرد (Cassese, 2005).

۳. تهدیدات سایبری علیه مراکز درمانی و بیمارستان ها

مراکز درمانی و بیمارستان‌ها نیز یکی از اهداف جدید حملات سایبری محسوب می‌شوند، چراکه دسترسی غیرمجاز به داده‌های بیماران، اختلال در تجهیزات پزشکی و قطع خدمات اورژانسی، می‌تواند تبعات جدی انسانی و اجتماعی داشته باشد حملات باج افزاری که در آن‌ها مهاجمان سیستم‌های بیمارستانی را رمزگذاری کرده و در ازای بازگرداندن اطلاعات، درخواست باج می‌کنند، در سطح جهانی به یکی از تهدیدات مهم تبدیل شده اند و ایران نیز از این حملات در امان نبوده است (Buzan, 1991).

د) تأثیر بر افکار عمومی و امنیت اجتماعی

حملات سایبری علاوه بر تأثیرات اقتصادی و نظامی، پیامدهای عمیقی بر افکار عمومی و امنیت اجتماعی دارند. در دنیای امروز، فضای مجازی به یکی از ابزارهای کلیدی برای شکل دهی به افکار عمومی، تأثیرگذاری بر نگرش‌های سیاسی و اجتماعی، و حتی برانگیختن نارضایتی‌های عمومی تبدیل شده است. جنگ اطلاعاتی و انتشار اخبار جعلی، بخشی از راهبردهای نوین جنگ سایبری محسوب می‌شوند که دولت‌ها و گروه‌های غیردولتی برای تغییر موازنه‌های قدرت از آن بهره می‌برند. جمهوری اسلامی ایران نیز در سال‌های اخیر، شاهد افزایش حملات سایبری با هدف تأثیرگذاری بر افکار عمومی و امنیت اجتماعی بوده است.

۱. جنگ اطلاعاتی و انتشار اخبار جعلی

یکی از مهم ترین ابزارهای تأثیرگذاری سایبری بر جوامع، انتشار اطلاعات نادرست و جعلی است که موجب تغییر نگرش عمومی و کاهش اعتماد شهروندان به نهادهای حاکمیتی می‌شود. گروه‌های سایبری با انتشار اخبار ساختگی، دستکاری داده‌های رسانه‌ای و گسترش روایت‌های کاذب، تلاش می‌کنند بر افکار عمومی تأثیر بگذارند و موجب بی ثباتی اجتماعی شوند. این نوع حملات در برخی موارد، همراه با نفوذ به حساب‌های کاربری مقامات و شخصیت‌های تأثیرگذار یا تغییر محتوای منتشرشده در رسانه‌های رسمی بوده است.

۲. حملات سایبری علیه شبکه‌های اجتماعی و رسانه ها

شبکه‌های اجتماعی و رسانه‌های دیجیتال، از جمله مهم ترین ابزارهای تأثیرگذاری بر افکار عمومی هستند و همین مسئله آن‌ها را به یکی از اهداف اصلی حملات سایبری تبدیل کرده است. نفوذ به شبکه‌های اجتماعی، هک حساب‌های تأثیرگذار و تغییر محتوای رسانه‌های رسمی، از جمله راهبردهای سایبری برای کنترل و هدایت افکار عمومی به شمار می‌رود. نمونه‌هایی از این حملات در سال‌های اخیر، منجر به پخش اطلاعات نادرست درباره مسائل حساس سیاسی و اقتصادی شده و به ایجاد ناآرامی‌های اجتماعی دامن زده است.

۳. تهدیدات سایبری علیه حریم خصوصی شهروندان

یکی دیگر از تأثیرات حملات سایبری بر امنیت اجتماعی، نقض حریم خصوصی شهروندان و سرقت اطلاعات شخصی آن‌ها است. حملات به سامانه‌های ارتباطی و نفوذ به پایگاه‌های داده اطلاعات کاربران، می‌تواند به ایجاد نگرانی‌های گسترده در جامعه منجر شود. نمونه‌هایی از این نوع حملات در برخی کشورها، باعث افشای اطلاعات کاربران شبکه‌های اجتماعی و پیام رسان‌ها شده که پیامدهای جدی برای امنیت اجتماعی و اعتماد عمومی داشته است.

PROOF VERSION

نتیجه‌گیری

امنیت سایبری در دنیای امروز دیگر صرفاً یک چالش فنی محسوب نمی‌شود، بلکه به یکی از مهم ترین مؤلفه‌های امنیت ملی تبدیل شده است. دیجیتالی شدن ساختارهای اقتصادی، دفاعی و اجتماعی، موجب افزایش آسیب پذیری کشورها در برابر تهدیدات سایبری شده است. جمهوری اسلامی ایران طی سال‌های اخیر هدف حملات گسترده‌ای در این حوزه بوده است که دامنه آن‌ها از حملات بدافزاری علیه تأسیسات هسته‌ای تا اختلال در زیرساخت‌های مالی و حمل ونقل عمومی را شامل می‌شود. بررسی این حملات نشان می‌دهد که تهدیدات سایبری نه تنها امنیت اطلاعات را به خطر می‌اندازند، بلکه می‌توانند موجب تضعیف امنیت دفاعی، بی ثباتی اقتصادی، اختلال در زیرساخت‌های حیاتی و ایجاد نارضایتی عمومی در جامعه شوند. یکی از مهم ترین پیامدهای تهدیدات سایبری، تأثیر آن‌ها بر امنیت دفاعی و نظامی کشور است. با توجه به وابستگی سامانه‌های فرماندهی، کنترل و تسلیحاتی به فناوری‌های سایبری، حملات سایبری می‌توانند موجب مختل شدن ارتباطات نظامی، سرقت اطلاعات راهبردی و حتی تغییر مسیر تسلیحات هوشمند شوند. حمله بدافزار استاکس نت نشان داد که تهدیدات سایبری می‌توانند فراتر از جنگ‌های اطلاعاتی، موجب ایجاد اختلال در سیستم‌های فیزیکی و صنایع استراتژیک شوند. در چنین شرایطی، توسعه سامانه‌های ارتباطی غیرمتمرکز، استفاده از رمزگذاری‌های پیشرفته و ایجاد شبکه‌های کنترل توزیع شده برای نیروهای مسلح، امری ضروری محسوب می‌شود.

علاوه بر تهدیدات نظامی، اقتصاد دیجیتال کشور نیز به شدت در معرض حملات سایبری قرار دارد. نفوذ به سامانه‌های مالی، سرقت اطلاعات بانکی و اختلال در سیستم‌های پرداخت الکترونیکی، موجب افزایش نااطمینانی اقتصادی و کاهش اعتماد عمومی به زیرساخت‌های مالی می‌شود. ایران طی سال‌های اخیر، شاهد حملاتی علیه بانک‌ها و بازارهای مالی خود بوده است که در برخی موارد، موجب افشای اطلاعات کاربران و ایجاد بی ثباتی در تراکنش‌های مالی شده است. به کارگیری فناوری‌هایی مانند بلاک چین، ایجاد سامانه‌های احراز هویت دیجیتال و استفاده از هوش مصنوعی برای شناسایی تهدیدات سایبری، از جمله راهکارهایی است که می‌تواند امنیت فضای اقتصادی دیجیتال را افزایش دهد. زیرساخت‌های حیاتی کشور نیز یکی از اهداف اصلی حملات سایبری محسوب می‌شوند. حملات به شبکه‌های توزیع برق، پالایشگاه‌های نفت، سیستم‌های حمل ونقل و مخابرات، می‌توانند موجب بروز بحران‌های ملی و اختلال در زندگی روزمره مردم شوند. برای مثال، حمله سایبری به شبکه راه آهن ایران و سامانه‌های توزیع سوخت در سال‌های اخیر، نشان داد که تهدیدات سایبری می‌توانند باعث بروز اختلالات گسترده و نارضایتی اجتماعی شوند. در چنین شرایطی، توسعه زیرساخت‌های مقاوم سازی شده، اجرای سیاست‌های پدافند غیرعامل در فضای سایبری و ایجاد سامانه‌های بازیابی سریع در زمان بحران، ضروری است.

جنگ سایبری صرفاً به حملات علیه زیرساخت‌های فنی محدود نمی‌شود، بلکه تأثیرات عمیقی بر افکار عمومی و امنیت اجتماعی دارد. عملیات‌های شناختی و انتشار اطلاعات جعلی از طریق رسانه‌های دیجیتال، می‌توانند موجب تغییر در نگرش عمومی، تضعیف اعتماد شهروندان به نهادهای حاکمیتی و حتی تحریک ناآرامی‌های اجتماعی شوند. در چنین شرایطی، افزایش سواد رسانه ای، تقویت سامانه‌های پایش اطلاعات فضای مجازی و مقابله با عملیات‌های اطلاعاتی دشمنان در فضای سایبری، امری ضروری است. با توجه به ماهیت چندلایه‌ای تهدیدات سایبری، جمهوری اسلامی ایران نیازمند اتخاذ یک راهبرد جامع برای تقویت امنیت سایبری خود است. توسعه فناوری‌های بومی، ایجاد شبکه‌های مقاوم در برابر حملات سایبری، بهبود تعاملات بین نهادی و افزایش همکاری‌های بین المللی، از جمله اقداماتی هستند که می‌توانند سطح امنیت سایبری کشور را افزایش دهند. بااین حال، یکی از مهم ترین ضعف‌های کشور در این حوزه، نبود یک مرکز واحد برای هماهنگی اقدامات امنیت سایبری در سطح ملی است. ازاین رو، ایجاد "مرکز ملی هماهنگی امنیت سایبری" که تمامی نهادهای دولتی، نظامی

PROOF VERSION

و خصوصی را تحت یک چارچوب یکپارچه برای تبادل اطلاعات تهدیدات سایبری و هماهنگی پاسخ‌های دفاعی قرار دهد، اقدامی حیاتی برای افزایش تاب آوری سایبری کشور محسوب می‌شود.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

موازین اخلاقی

در انجام این پژوهش تمامی موازین و اصول اخلاقی رعایت گردیده است.

شفافیت داده‌ها

داده‌ها و مآخذ پژوهش حاضر در صورت درخواست از نویسنده مسئول و ضمن رعایت اصول کپی رایت ارسال خواهد شد.

حامی مالی

این پژوهش حامی مالی نداشته است.

References

Abdollah Khani, A. (2003). *Security Theories: An Introduction to National Security Doctrine Planning (Volume 1)*. Abrar Contemporary Cultural Studies and Research Institute.

Ahmadinejad, H. (2010). *NATO's Presence in Iran's Surrounding Environment and the National Security of the Islamic Republic of Iran* Allameh Tabataba'i University, Faculty of Law and Political Science].

Ahmed Jamal, A. (2021). A Review on Security Analysis of Cyber Physical Systems Using Machine Learning. *Materials Today: Proceedings*.

Alghamdi, M. I. (2021). Determining the Impact of Cyber Security Awareness on Employee Behaviour: A Case of Saudi Arabia. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.04.093

Baman Eghbali Zarch, A. (2022). *Cyber Threats and Attacks Against Iran*. Institute for Political and International Studies (IPIS).

Beaumont, P. (2010). US Appoints First Cyber Warfare General. *The Observer*, 10.

Brenner, S. W., & Clarke, L. L. (2010). Civilians in Cyberwarfare: Conscripts. *Vanderbilt Journal of Transnational Law*, *43*, 1011-1076.

Buzan, B. (1991). New Patterns of Global Security in the First-Twenty Century. *International Affairs*, *67*(3), 431-451. https://doi.org/10.2307/2621945

Buzan, B. (1999). *People, States, and Fear*. Strategic Studies Research Institute.

Cassese, A. (2005). *International Law*. Oxford University Press.

Castells, M. (2010). *The Information Age: Economy, Society, and Culture*. Tarh-e No.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review*, *27*(3), 221-XXX. https://doi.org/10.1177/0192512106064462

Hare, F. (2010). *The Cyber Threat to National Security: Why Can't We Agree?* CCD COE Publications.

Kizza, J. M. (2007). *Ethical and Social Issues in the Information Age*. Springer-Verlag.

PROOF VERSION

Krishnasamy, V., & Venkatachalam, S. (2021). An Efficient Data Flow Material Model-Based Cloud Authentication Data Security and Reduce a Cloud Storage Cost Using Index-Level Boundary Pattern Convergent Encryption Algorithm. *Materials Today: Proceedings*. https://www.sciencedirect.com

Liu, X., Zhang, J., Zhu, P., Tan, Q., & Yin, W. (2021). Quantitative Cyber-Physical Security Analysis Methodology for Industrial Control Systems Based on Incomplete Information Bayesian Game. *Computers & Security*, *102*, 102138. https://doi.org/10.1016/j.cose.2020.102138

Mandel, R. (2008). *The Changing Face of National Security*. Strategic Studies Research Institute.

Rosenau, J. (2011). *The Information Revolution, Security, and New Technologies*. Strategic Studies Research Institute.

Sayyad, M. K., Amini, A., & Taheri, A. (2020). Cyber Threats and Security Measures in Virtual Space: A Comparative Study of the Approaches of the United States and the Islamic Republic of Iran. *National Security Scientific Quarterly*, *10*(38), 293-331.

Starr, S. H. (2009). Towards an Evolving Theory of Cyber Power. *National Defense University, Center for Technology and National Security Policy*. https://doi.org/10.3233/978-1-60750-060-5-18

Talebpour, A. (2019). *A History of Cyber Attacks in Iran and the World*. Young Journalists Club News Agency.

Torabi, G. (2018). Challenges and Vulnerabilities of the Islamic Republic of Iran in Cyberspace. *Strategic Studies*, *21*(1), 167-195.

PROOF VERSION